

AO 91 (Rev. 11/11) Criminal Complaint

SealedPublic and unofficial staff access
to this instrument are
prohibited by court order.

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States Court
Southern District of Texas
FILED

JUN 22 2018

David J. Bradley, Clerk of Court

United States of America

v.

Derrick Ervin

Case No.

H18-1007M

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of See offense description below in the county of Brazos in the
Southern District of Texas, the defendant(s) violated:

Code Section

Offense Description

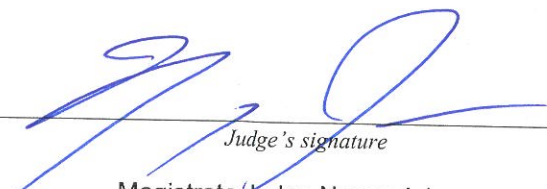
In or about March 2018, within the Southern District of Texas, the Derrick Ervin, did knowingly combine, conspire, confederate and agree with others known and unknown to the Grand Jury, to commit the offense of wire fraud against the United States, in violation of 18 USC 371

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.
Complainant's signaturePerry E. Wilson FBI-SA
Printed name and title

Sworn to before me and signed in my presence.

Date: 6-22-18City and state: Houston, Texas
Judge's signature
Magistrate Judge Nancy Johnson
Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR AN ARREST WARRANT**

I, Perry E. Wilson, being first duly sworn, hereby depose and state as follows:

SUMMARY

The FBI, in partnership with City of Bryan (TX) Police Department, has been investigating a business email compromise. Essentially, people posing as vendors of the City of Bryan sent emails directing the City to wire money to their “new” bank accounts. In reality, however, these accounts were actually controlled by conspirators who then transmitted the money further downstream. The FBI seeks to arrest Derrick Ervin, one of these conspirators and submits there is probable cause to believe that he has violated 18 U.S.C. § 371 (conspiracy to commit wire fraud).

INTRODUCTION AND AGENT BACKGROUND

1. I am an FBI Special Agent assigned to the Houston Field Office, Bryan Resident Agency. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. § 2510(7), as a Special Agent of the FBI. As such, I am empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516, including 18 U.S.C. §§ 371, 1028A, 1029, 1030, 1343, 1344, and others.
2. I have been employed as a Special Agent since May 2006. As a Special Agent of the FBI, I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. I investigate crimes involving wire and bank fraud, business email compromises, and financially motivated crimes. I have worked a variety of matters, including, but not limited to, wire and mail fraud, money

laundering, as well as matters that included a significant cyber component. I have training in the preparation, presentation, and service of criminal arrest and search warrants, and have been involved in the investigation of offenses against the United States.

3. Based on my training and experience, I have learned that individuals involved in identity theft-related bank fraud and wire fraud schemes and/or computer intrusions employ a number of sophisticated techniques, either singly or in combination, to further their illegal activities and to avoid detection by law enforcement. These techniques can include utilizing web-based e-mail accounts and other electronic messaging accounts to send, receive, store, and obtain personal identifying information, such as Social Security numbers, dates of birth, and bank and credit card account numbers and related information; utilizing software programs or “spoof” websites or e-mail messages to dupe e-mail recipients and others into downloading malicious software aimed at tracking and causing those individuals to unwittingly reveal or provide their personal identifying information; using computers, servers, and other electronic devices to commit computer intrusions, manufacture false identification documents and financial transactions cards, and a variety of other methods in furtherance of their schemes.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. In particular, I also rely on information provided to me by Beau Wallace of the City of Bryan (Texas) Police Department. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts in this affidavit, I submit there is probable cause to believe that Derrick Ervin has violated 18 U.S.C. § 371 (conspiracy to commit wire fraud) (the “Subject Offense”).

PROBABLE CAUSE

Background

6. The FBI is investigating a business email compromise that targeted the City of Bryan, Texas. The City of Bryan is an incorporated municipality in Brazos County, in the State of Texas. As such, they routinely do business with vendors and contractors that provide services to the city and are thereafter reimbursed for those services.

7. A business email compromise (BEC) is defined as a scheme to defraud targeted businesses working with vendors and/or businesses that regularly perform wire transfer payments or ACH transfers. The scam takes several forms, but typically involves the use of fraudulent “spoofed” email addresses, confusingly similar domains and/or hacked email accounts to invent a fictitious transaction, or hijack a legitimate one, in an effort to misdirect the funds. BECs typically culminate in the fraudsters sending fraudulent wiring instructions to a financial institution or other business directing the transfer of a large sum of funds to a bank account controlled by the fraudsters, on various pretenses (e.g., that the account belongs to the seller or intermediary acting on its behalf, or that the sender of the instructions is an employee of the corporate account holder with authority to authorize wire transfers on its behalf).

The City of Bryan suffers a business email compromise

8. In this case, in March 2018, the suspect(s) posed as business partners (such as vendors) of the corporate victim (in this case the City of Bryan), and sent fraudulent emails

from a confusingly similar domain, saying that the so-called vendor had changed banks, and asked that payments be sent to a new bank account. The City of Bryan thought they were paying their vendors, but in reality, the vendors had no idea these emails were sent, and the city was being defrauded.

9. On or about March 16, 2018, the City of Bryan, Texas became aware they had been victims of a business email compromise scheme. In the weeks preceding, unknown subjects had sent falsified Electronic Funds Transfer (EFT) forms to the City of Bryan, updating legitimate vendor payment information. The City of Bryan updated the vendor information and sent payments to the suspect(s) instead of the actual vendor. A total of three wire payments were sent. They are as follows:

- (1) \$358,835.09 on 3/9/18 to Larry Young Paving to a Chase Bank account (xxxxx6633)
- (2) \$382,111.71 on 3/9/18 to LDF Construction to an Investors Bank account
- (3) \$38,860.70 on 3/16/18 to Larry Young Paving to the same Chase account (xxxxx6633)

9. City of Bryan discovered the fraud when the payment to LDF Construction went into a new banking account with Investor's Bank in New Jersey. Staff with Investor's Bank were approached in the branch and asked to wire the whole amount elsewhere. They thought the initial wire and request were suspicious so they placed a hold on the remaining amount while they investigated. They contacted the City of Bryan where it was then discovered the EFT forms had been falsified.

10. City of Bryan staff then conducted an audit and learned there was another EFT form that had been updated without the proper protocols being followed. They learned two payments to Larry Young Paving had also been sent to the suspect(s). The suspect created

confusingly similar e-mail domains that tricked City of Bryan personnel into thinking it was the real vendor.

\$197,000 was received by Bank of America account 6165 opened by someone who used the identity of “Jayme E. Porter”

11. The funds sent into the Chase account (xxxxxx6633) account were traced through numerous accounts opened in the names of people other than Ervin. Of the approximately \$390,000 sent into the Chase Bank account (xxxxxx6633), a wire for just over \$197,000 was sent to a Bank of America account (xxxxxxxxx6165).

12. Information provided by Bank of America indicated the account name in which the funds were placed was Triton Equipment Distribution LLC,¹ with the sole signor on this LLC’s behalf being a “Jayme E. Porter.”

13. Per Bank of America, “Porter” used Pennsylvania Driver’s License (DL) 83734817 to open the account and provided 7/25/1983 as their Date of Birth (DOB). A check of that name and Pennsylvania Driver’s License was performed. The license number was not valid. However, the name and DOB provided by Bank of America matched a Jayme Elizabeth Porter, a white female in her mid-30s who resided in Philadelphia (picture below). Despite this fact, the account was opened on 1/11/18 at a branch at Marietta, Georgia.

¹ Bank of America records also reflect the following information for Triton Equipment Distribution LLC as 315 W Ponce De Leon Ave. Suite 235, Decatur, GA 30030-2483 and the tax ID as 82-3283192. The phone number provided was 404-430-9406. This address is discussed further below.



14. According to Bank of America, the e-mail address provided for the bank account was j.porter0725@gmail.com.

The Gmail account given to Bank of America was created using an IP address opened by Derrick Ervin

15. Records obtained from Google for j.porter0725@gmail.com showed the account was opened on 11/02/17 at 00:57 UTC using IP address 2601:c1:c100:372a:c86b:c1c7:bfcf:1504. Investigation into that IP address indicated it belonged to Comcast.

16. Records were obtained from Comcast for this IP address during the time of the Google account creation. Around May 30, 2018, Comcast responded with the following information:

Subscriber Name: Derrick Ervin
Service Address: 2030 Main St NW APT 306, Atlanta, GA 30318-1877
Telephone Number: 404.358.1381
Type of Service: High Speed Internet Service
Account Number: 8220188950878298
Start of Service: Connected 09/21/15, Disconnected 11/29/17,
Reconnected 12/04/17
Account Status: Active
IP Assignment: Dynamically Assigned

Bank of America security camera footage corroborates that the person who used Jayme E. Porter's information to open that bank account was actually Derrick Ervin

17. Bank of America provided security camera footage to show the person who conducted the transactions on the Triton Equipment Distribution/ Jayme Porter account. A comparison of the subject in the surveillance videos and the Georgia Driver's license photo of Derrick Ervin show what appears to be the same individual.

18. For example, here is Ervin's Georgia driver's license 053709538 photo:



19. Similarly, here is bank footage from around January 11, 2018 1456 hours at 3030 Windy Hill Rd., Marietta, GA 30067 when the Bank of America account 6165 was opened:



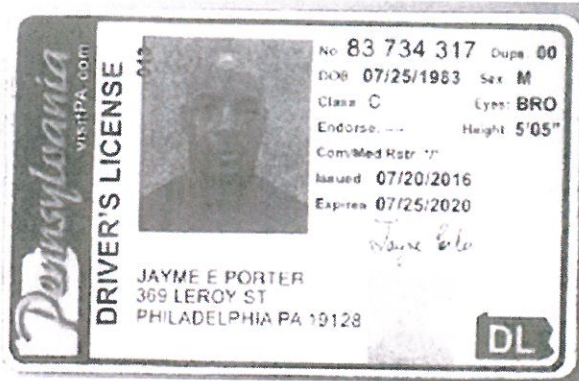
20. Similarly, here is bank security camera footage of the person who, around March 14, 2018 at 1520 hours at 1 Perimeter CTR E, Atlanta, GA 30346 – drained the account of the money received that was traced to the City of Bryan business email compromise.



21. In contrast, records checks show that Jayme E. Porter with date of birth 7/25/83 who resides in Pennsylvania appears to be a Caucasian female in her mid-30s.

Ervin also used Jayme E. Porter's identifying information when he opened a P.O. Box in March 2018

22. Ervin appears to be difficult person to locate. Records were obtained from The UPS Store at 2451 Cumberland Parkway, Atlanta, GA for P.O. Box 345. This box was opened on March 21, 2018 by Ervin who provided the name Jayme Porter and the following driver's license which contains the real Jayme E. Porter's name, address, and date of birth – but with Ervin's picture.



23. First, as noted above, he apparently opened Bank of America account 6165 using the identity of Jayme Porter. Second, the FBI has started to look for him using CLEAR (similar to Accurant or TLO), and it appears that he uses multiple Social Security Numbers and addresses. Similarly, his last driver's license listed his address as 5200 Suttles Drive SW, Atlanta, which appears to possibly be a townhouse. Comcast records listed him at 2030 Main St NW in Atlanta, Apt. 306 which appears to be a townhouse as well. The address 10411 Tobano Trail in Jonesboro, GA is listed as an associated address.

In March 2018, Derrick Ervin quickly drained Bank of America account 6165 of money received as a result of the City of Bryan business email compromise

24. On March 9, 2018, the City of Bryan was tricked into wiring \$358,835.09 to Chase Bank account 6633.

25. On March 13, 2018, Chase Bank account 6633 wired \$197,590.00 to Ervin's Bank of America account 6165, according to Bank of America records.

26. Ervin quickly acted to drain this account. On March 14, 2018, Ervin conducted four transactions that withdrew \$195,200 from the account:

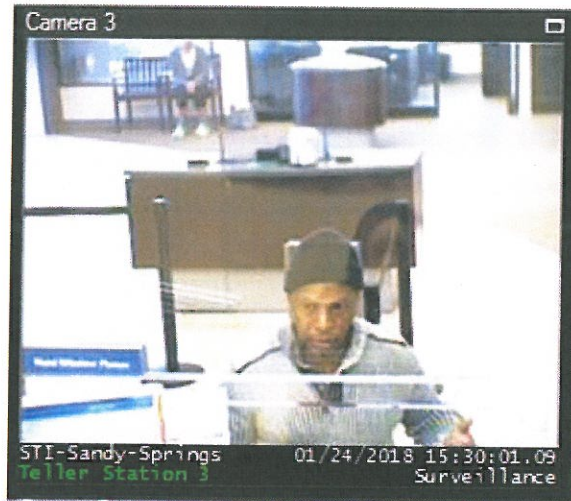
1. He cashed a \$28,500 check made payable to "Cash."
2. He obtained cashier's check no. 934218114 for \$67,700.00.
3. He obtained cashier's check no. 934218115 for \$42,800.00.
4. He obtained cashier's check no. 934218116 for \$56,200.00.

27. In addition, the next day, he made a \$533.61 purchase at Louis Vuitton in Atlanta, GA.

Ervin also uses Jayme Porter's information to open at least one other bank account in January 2018

28. This is not the only time that Ervin has stolen money using Jayme Porter's identity. Our investigation has also revealed a similar scheme in which money was sent to SunTrust account 8230 (again, I only include the last four digits of the account number, although the full number is known to the FBI) – also opened under the name Triton Equipment Distribution LLC.

29. As with the Bank of America account, the SunTrust Triton Equipment Distribution account 8230 was opened around January 11, 2018 with the sole signor as "Jayme E. Porter." Again, however, security camera footage was obtained showing Ervin, acting as Porter, depositing a Triton Equipment Distribution SunTrust check, endorsed by a "Jayme Porter" signature, into the Triton Equipment Distribution Bank of America account. Further, the images below are from a SunTrust Bank, showing that the "Jayme Porter" making a \$12,000 withdrawal from the SunTrust account in January 2018 was Derrick Ervin.



TRAINING AND EXPERIENCE

30. Based on my training, my experience and this investigation, I know the following:

31. People who engage in the Subject Offense frequently do so with the assistance or cooperation of others. Indeed, I understand that business email compromises often involve multiple people, both to send the victim fraudulent emails, as well as those downstream who are tasked with receiving the money and withdrawing it before the victim can cancel the transaction.

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- c. Digital device includes computers and storage media.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

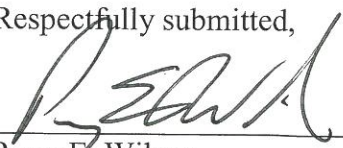
- e. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

Under Internet Protocol version 4, an IP address looked like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). However, to accommodate the need for more IP addresses, Internet Protocol version 6 lists an IP address using the format of 8 groups of 16 bits each. Each group is written as four hexadecimal digits (sometimes called hextets) and the groups are separated by colons. One example is 2601:c1:c100:372a:c86b:c1c7:bfcf:1504.

- f. “Records” and “information” include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

For these reasons, I ask the Court to authorize this arrest warrant.

Respectfully submitted,


Perry E. Wilson
FBI Special Agent

Subscribed and sworn to before me on June 22, 2018.


UNITED STATES MAGISTRATE JUDGE